IHS Division of Information Security

Audit and Assist Team

Mike Ginn and Ryan Chapman

IHS Technology Conference, June 2006

Agenda

- Audit and Assist process
- Security Controls
- Federal Regulations
- Tools Used
- Best Practices
- Trends
- Future plans

Team Members

- Mike Ginn
- Ryan Chapman (Analex Contractor)
- Nick Pappas (Analex Contractor)

Purpose

- The Team assists facilities with their information security responsibilities. We review systems and processes for compliance with federal legislation, directives, policies, and procedures.

Workflow

1. Pre Assist (3-4 weeks before onsite visit)

2. Onsite visit (2-4 days depending on size of the facility)

3. Post Assist (4-6 weeks after onsite visit)

Pre Assist Phase (logistics)

- Contact Area ISSO
  - Looking for suggestions for sites
  - Go over our schedule
- Contact Site Manager, Service Unit Director, ISC, and Area Director
  - To get approval and agree on logistics (dates of site visit)

Pre Assist Phase (continued)

- Pre Assist packet - to the site requesting information from them
- Short survey asking:
  - # of desktops/laptops
  - Types of operating systems
  - POC(s) for people who maintain the documentation for:
    - Computer Access Forms
    - Rules of Behavior
    - Clearance of Separation

Pre Assist Phase (continued)

- Notifying them of things we will require
  - Space to work for 3 people
  - Administrator access
  - Availability of key personnel

Pre Assist Phase (continued)

- Asking if the facility has:
  - A Security Plan
  - COOP
  - Incident Response
  - Risk Assessment
  - C & A
- And if so we ask them to give us copies so we can evaluate them (preferably electronic).

Pre Assist Phase (continued)

- Also asking for copies of:
  - Network diagrams
  - System Specifications
  - List of recently separated employees
  - Authorized software
  - Standard configurations

Pre Assist Phase (continued)

- Once we receive the packet back at OIT we take a couple of weeks to review it and determine our plan:
  - How much time we will need
  - Review vulnerabilities (macintosh, wireless, etc.)

Site Visit Phase

- Start out with initial presentation to SUD and IT staff
  - Introductions
  - What we will be doing
  - How long we will be there
  - How findings will be communicated
  - Ask about any concerns they have

Site Visit Phase (continued)

- Walk through of facility, outlying facilities
- Plug in a sniffer – start capturing traffic
- Review (5%) amount of Desktops and Laptops.
- Interview (5%) system users (laptop, handheld, managers)
- Review documentation on file

Site Visit Phase (continued)

- Working through our checklists
- Conduct interviews with users, managers, people who maintain documentation, security guards, building manager, etc.
- Assist in mitigating weaknesses discovered
  - Forms
  - How to read logs
  - Upgrade to NAV 10, or tell them about HFNETCHK

Site Visit Phase (continued)

- Exit brief session at end of visit with SUD and IT Staff
  - Findings – with recommendations that need to be taken care of ASAP
  - When to expect final report - Combination of technical recommendations and observations

Post Assist Phase

- Take all of our findings back to OIT
- Develop final report
- Deliver final report to SUD, ISSO, ISC, and Site Manager
- Ask for feedback – thru “Feedback Survey”
- At this same time, we are doing the pre assist work for the next site.

Post Assist Phase (continued)

- Findings Report
  - We report any critical weaknesses in the exit brief. But all weaknesses are included in the written report with suggestions for corrective action. We write it in terms that are understandable to people who might have limited IT expertise.
  - This information helps senior management understand the significance of the weaknesses and importance of taking corrective actions.
  - All of our findings are broken down into either:

    Immediate Action Required

    Action Required

    No Action Required

Checklists

- Desktop Configurations
- Servers and Gateways
- System Administrator Interview
- Documentation
- Physical Security
- Building Management. Interview
- Management Interview
- Observations
- General Users/Laptop Users/Handheld Users

Checklists (continued)

- Can trace all the checklist items and expected results to one of the following:
  - HHS Guidelines
  - IHS SOPs
  - NIST 800-53 - Recommended Security Controls for Federal Information Systems
  - FISCAM – Federal Information Systems Controls Audit Manual

Some of the tools used

- Nmap
- Nessus
- NIKTO
- Netstumbler/Kismet

Best Practices

- Security Guards incorporating Computer Security in daily rounds
- Site managers trying out anti-spam/spyware applications
- Employee would not let us in their office (confidential info)
- Wyse/terminal services
- Penetration Tests, physical in addition to network
- Ryan: a couple more – BUS book, using waivers, backups by area office at night

“Not so best” Practices

- Computer access forms
- Wireless widely deployed but not FIPS compliant
- Shared access codes and passwords
- Non-IHS computer on IHS network without security controls.
- Windows 98 (even 95) still being used.
- Incident Response
- Site managers uninformed about D1
- Reviewing Logs – not happening
- ???? Site managers unsure how to get rid of hard drives?????

Upcoming Trends

- Electronic Health Record (EHR)
- Wireless networking
- Centralized management – Network Operations and Security Center (NOSC)
- Configuration Management
- Voice Over IP (VOIP), IP Telephony
- Telemedicine, i.e.
- Smart Cards, aka HSPD-12 & Public Key Infrastructure (PKI)
- Ever greater accountability for Confidentiality, Integrity and Availability (CIA)

Future Plans for Audit & Assist Team

- Continue revising checklists and methodology based on feedback and new/revised IHS/HHS policies.
- Develop checklists for servers, routers, RPMS
- Next site visits will likely be in Billings and Bemidji Areas.
- We are open to suggestions if someone has a site they would like us to visit.

Availability

- The Team is available for Site visits this summer.
- There is no cost to the Area Office or Service Units.
- If you would like to talk more about the process or schedule the Team for a visit:
  - Mike: 505-248-4787
  - Ryan/Nick: 505-248-4390
  - Email: OITAuditAssistTeam@ihs.gov

QUESTIONS?